The Operational Impacts of the Global Network Enterprise Construct

A Monograph
by
Major John Nelson
USA

School of Advanced Military Studies
United States Army Command and General Staff College
Fort Leavenworth, Kansas

AY 2010

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE (DD-MM-YYYY) 14-05-2010	**2. REPORT TYPE** SAMS Monograph	**3. DATES COVERED** *(From - To)* July 2009 – May 2010

4. TITLE AND SUBTITLE
The Operational Impacts of the Global Network Enterprise Construct

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Major John E. Nelson (U.S. Army)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
School of Advanced Military Studies (SAMS)
250 Gibbon Avenue
Fort Leavenworth, KS 66027-2134

8. PERFORMING ORG REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Foreign Military Studies Office & Command and General Staff College
Director, FMSO
731 McClellan Ave.
Fort Leavenworth, KS 66027-1350

10. SPONSOR/MONITOR'S ACRONYM(S)
FMSO / CGSC

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The purpose of this monograph is to examine the operational impacts of the Army's transformation of network enterprise management on the signal community, particularly the impacts upon Division and Corps G6 personnel. The Global Network Enterprise Construct will dramatically change the manner in which the Army draws enterprise services; in order for the transformation to be successful in attaining its goals, the signal community must take into account the impacts the transformation will have on the war fighters.

The methodology of this paper is to first examine the Global Network Enterprise Construct in the context of how the Army managed networks in the past. This study traces the governmental and Department of Defense policies that the construct supports. The study outlines how the signal community expects to complete the transformation by 2015. Finally, it examines the lone operational deployment of a brigade supported by the construct followed by what the possible points of future friction are for the signal community as they transform Army enterprise management.

15. SUBJECT TERMS
Global Network Enterprise Construct, Network Management, Signal Corps, Chief Information Officer, Army Network Enterprise Command.

16. SECURITY CLASSIFICATION OF: **(U)**			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** Stefan J. Banach COL, U.S. Army
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. PHONE NUMBER** *(include area code)*
(U)	(U)	(U)	(U)	80	913-758-3302

SCHOOL OF ADVANCED MILITARY STUDIES
MONOGRAPH APPROVAL
Major John E. Nelson
Title of Monograph: The Operational Impacts of the Global Network Enterprise Construct
Approved by:

__________________________________ Monograph Director
Robert T. Davis, PhD

__________________________________ Monograph Reader
Bruce E. Stanley, Seminar Leader

__________________________________ Director,
Stefan Banach, COL, IN School of Advanced
Military Studies

__________________________________ Director,
Robert F. Baumann, Ph.D. Graduate Degree
Programs

Disclaimer: Opinions, conclusions, and recommendations expressed or implied within are solely those of the author, and do not represent the views of the US Army School of Advanced Military Studies, the US Army Command and General Staff College, the United States Army, the Department of Defense, or any other US government agency. Cleared for public release: distribution unlimited.

Abstract

THE OPERATIONAL IMPACTS OF THE GLOBAL NETWORK ENTERPRISE CONSTRUCT, by Major John Nelson.

The purpose of this monograph is to examine the operational impacts of the Army's transformation of network enterprise management on the signal community, particularly the impacts upon Division and Corps G6 personnel. The Global Network Enterprise Construct will dramatically change the manner in which the Army draws enterprise services; in order for the transformation to be successful in attaining its goals, the signal community must take into account the impacts the transformation will have on the war fighters.

The methodology of this paper is to first examine the Global Network Enterprise Construct in the context of how the Army managed networks in the past. This study traces the governmental and Department of Defense policies that the construct supports. The study outlines how the signal community expects to complete the transformation by 2015. Finally, it examines the lone operational deployment of a brigade supported by the construct followed by what the possible points of future friction are for the signal community as they transform Army enterprise management.

Table of Contents

Introduction

The Global Network Enterprise Construct (GNEC) is the Army's effort to manage service networks and applications as a single enterprise. The Chief of Staff of the Army, GEN George Casey, approved the GNEC concept in March 2009. The construct, through the development of Network Service Centers (NSC) will transform the Army's current network support structure from a diversified organizationally based structure to a centralized structure. The anticipated results of the GNEC transformation are enhanced mobility, cost saving and improved cyber security through better network visibility. Additionally, GNEC will enable units to utilize the same applications in garrison as they do during an operational deployment. The Army Chief Information Officer/G6 (CIO/G6) is responsible for implementing the plan. With GNEC, the United States Army Network Command (NETCOM) will be responsible for providing all enterprise service support to the force.

As personal computing technology emerged in the late eighties, the Army proponent for managing it was the Information Systems Command (ISC). The proliferation of computers and networks across Army institutions quickly out paced ISC's ability to manage. The ISC was disbanded and the local garrison commanders assumed the ISC's role. Directorate of Information Management (DOIM) organizations serving the garrison commander supported the networking needs of each installation. Concurrently, individual organizations on each installation also established and managed unit networks and services. Although some regulations were in place to govern these diverse and individual networks, validating that these networks were following regulations was difficult. Each installation operated their network in accordance with the desires of the customers they supported: this system of network management posses many problems.

The decentralized nature of the organizational system of network management leads to security vulnerability.[1] Lacking the capability to see the entire network, the Army's network operations service centers were unable to adequately ensure that the Army's networks were secure. Further, individual organizations were responsible for validating their own security requirements. The decentralized system also resulted in a wide variety of network hardware and software on the Army's global network. The DOIMs at each installation were responsible for administering the installation's network. United States Army Signal Command (ASC) was the organization responsible for the Army's data network throughout the early nineties. Each DOIM reported to them on technical and certification issues, but the DOIMs served the garrison commander. As a result, the ASC's ability to effectively manage and secure the Army's network was compromised.

This system of network management persisted until 2002. The establishment of NETCOM as the single authority for providing network support and enterprise services transferred the DOIMs to the operational control of NETCOM. Further, NETCOM began to federate all DOIMs in the continental United States (CONUS). Each DOIM first became the only enterprise service provider in garrison. All unit level networks and enterprise service suites were eliminated in garrison, but were still used during operational deployments. This led, by 2003, to each installation owning it's own domain. While the situation had improved, establishing trusts between these domains and ensuring connectivity between them remained a problem. By 2007, each of the DOIMs had consolidated their separate domains into Combatant Command domains. This streamlined network management by significantly decreasing the amount of domains that

[1] There are two approaches to cyber security with regards to protecting closed networks. The first holds that a smaller network is more secure as a result of the limited amount of users presents less opportunity for network intrusions. The counter argument, which the Army supports, is that a large network is more secured in that the security personnel can see the entire network and detect and counter any intrusions quickly.

needed to be connected. Further, it made it possible for the Network Operations Service Centers to better see and protect the Army's network.

In addition to the institutional network, NETCOM is also responsible for the operational network. When a unit leaves garrison for an operational deployment, it leaves the institutional network. While deployed, brigade and above headquarters establish their own domains and enterprise services. As a result, in a theater such as Iraq, a tremendous amount of domains exists, leading to the same security and management problems seen in the past. Further, a unit on the institutional network does not have the same services they will have while deployed. These dual networks also result in each user on the systems having two on-line identities. To merge the institutional and operational networks, the CIO/G6 initiated the GNEC campaign plan in 2009.

GNEC will use Network Support Centers, consisting of Area Processing Centers, Tactical Network Operations Centers and Fixed Regional Hub Nodes to bring the operational network in line with the institutional network. Instead of each unit establishing its own domain and enterprise services, the unit will only provide the communications link to the Regional Hub. All enterprise support systems will be located and managed from the Area Processing Centers. These centers will host the unit's services full time, both in garrison and while deployed. In this manner, NETCOM will provide plug and play capability to the war fighters. GNEC will also eliminate the redundancy of two networks and ensure that forces have the same capabilities and access while training in garrison for deployment. Further, this will streamline the Army's network and enable centralized control in order to better see and protect the network.

GNEC hopes to achieve one truly global network with an infrastructure that is invisible to the user. This goal will be difficult to achieve given current the Army's current communications systems. During the only test of the construct to date, Operation Validation, significant shortfalls were evident in transport capacity, migrating between phases and network command and control. The exercise notionally deployed a brigade from Fort Bragg to Europe. The Fort Bragg Area Processing Center managed the brigade's enterprise services. Despite the shortfalls mentioned above, the construct was effective in providing data support to the brigade. The larger implications of GNEC is the loss of a capability within the brigade and higher headquarters. The G6 personnel within the headquarters will lose their servers, as the processing centers will host these services. Any time a unit needs to add or alter their service, they must request the changes through the Network Operations Service Center and await first approval and then application of the changes. No longer will the corps and division G6 have sole responsibility for managing their domains. In the future, the unit will simply establish a link to the hub and plug in. Any changes to the unit's services or outages can only be addressed by the Network Operations Center. The loss of this capacity may be an issue with commanders who are satisfied with the current institutional and operational networks.

In order for GNEC to be successful, the signal community must ensure they have established trust with their clients. It is difficult to relinquish a resource and trust that someone else will do as good a job as your own people. With clearly expressed rules of governance, proactive customer service and reliable and flexible network support the signal community can build that trust. Additionally, new equipment is necessary to realize all of the goals of the construct. In order to push data services to the company level, brigade communications equipment must change drastically. Current communications assemblages within an Army brigade are only capable of pushing data support to the battalion level. Further, some of these assemblages do not support all of the data services typically used in the Army, such as teleconferencing. In order to attain the goals of GNEC, the signal community must ensure they can adequately support the war fighter.

Unlike prior attempts at network management, the GNEC campaign has tremendous potential to succeed. The lessons learned in applying a consolidated, processing center hosted institutional network on garrisons in the United States will be invaluable in applying this same construct to the deployed network. Since 2001, the Army has been consolidating services within the garrison environment. Consolidating all services at the Directorate of Information

Management was complete in 2007. Since then, the Army has federated many of the installation networks into major command enclaves. The approach used to consolidate network and enterprise services on the garrison network will prove sufficient to consolidate the deployed network.

GNEC is essential to efficiently protect the network and to adequately support the force. The only way it will fail is if during the transition, the signal community fails to adequately support their clients. If the force loses faith in the new system, they will hold with the current system, which adequately supports their needs.

Literature Review

The transition to a global enterprise construct has its roots in the *Army Knowledge Management Guidance Memo 1* of 2001. Both the Chief of Staff of the Army, GEN Eric Shinseki and the Secretary of the Army, the Honorable Mr. Thomas White signed this memo. This memo laid out the Army leadership's goals on Knowledge Management. The goals are: adopt governance and cultural changes to become a knowledge based organization, integrate knowledge management and best business practices into Army processes, manage the infrastructure at the enterprise level while consolidating infrastructure, scale Army Knowledge On-line as the enterprise portal, and harness human capital for the knowledge organization. In practical terms, the memo also mandated Major Commands and other Army organizations must receive CIO/G6 approval for all information management and information technologies acquisitions. Further, all organizations were to begin planning for server and enterprise service consolidation. The stated goal of the memo was to create a network centric, knowledge based force with an enterprise vision of a single Army network with one portal and universal access.[2]

In 2002, *The Army Knowledge Management Guidance Memo #2* updated and reinforced the 2001 guidance. It reiterated the Army Leadership's commitment to creating a network centric and knowledge based organization. The memo also provided guidance that dictated server consolidation and designated responsibilities to both Directorate of Information Management (DOIM) and the Army Chief Information Officer/G6 (CIO/G6). The DOIMs assumed responsibility for network security at the installation level and the CIO was charged with forming an executive board to oversee and manage the Army Knowledge On-line (AKO) web portal.[3] This was the last Army Knowledge memo to be released by the Secretary and Chief of Staff.

[2] Department of the Army, *Army Knowledge Management Guidance Memo #1*, (Washington D.C.: Government Printing Office, 2001).

[3] Department of the Army, *Army Knowledge Management Guidance Memo #2*,"(Washington D.C.: Government Printing Office, 2001).

The Department of the Army released the *Army Knowledge Management Implementation Plan* in 2003. This document served as an update on the implementation of the goals expressed in Memo 1. It served two purposes: to identify critical enablers necessary to achieve the vision of a net centric and knowledge-based force and to find the "irreversible momentum," those initiatives that support the Army Knowledge Management Strategy. The plan also provided an update on the goals of knowledge management: governance, best practices, infrastructure, AKO and human capital. Each of these goals served as a category under which were several smaller tasks. Such as standards and accredidation falling under governance. There, the document provided an update on what standards were available and which organization was responsible for producing and implementing them.[4]

The *Single DOIM Action Plan for Command, Control, Communications, Computers and Information Management (C4IM) Common User Services* was the next substantive document governing network management. The Department of the Army published it in March of 2006. This document specifically dictates the roles and responsibilities of the installation DOIM. First, the installation DOIM was to consolidate all C4IM on the installation; further, the DOIM would technically validate all installation tenant organizations information technology acquisitions. The goal of the action plan was to work towards achieving one Army network that permits users to access authorized network resources regardless of the location of the resource or of the user. The plan did not apply to DOIMs located overseas nor did the plan apply to deployed forces.[5]

Although it had its roots in 2006, Training and Doctrine Command (TRADOC) released the *U.S. Army Concept of Operations LandWarNet 2015* in 2008. The document details the future requirements LandWarNet will have to provide the war fighter. Although it is a plan for the

[4] Department of the Army, *The Army Knowledge Management Implementation Plan*, (Washington, D.C.: 2003).

[5] Department of the Army, The Single DOIM Action Plan for Command, Control, Communications, Computers and Information Management (C4IM) Common User Services, (Washington, D.C.: Government Printing Office, 2006).

future, the pamphlet is careful to express early on that LandWarNet is not new or in development, it has existed for years and it represents the Army's portion of the Global Information Grid (GIG). LandWarNet is all of the Army's information technology resources, including transport, management, data and applications. The concept of operations provides a comprehensive view of the capabilities the network must provide to enable the war fighter. It specifically addresses how LandWarNet must be deployed, fielded and managed to address diverse threats and volatile conditions throughout the joint phased network. LandWarNet must enable see, move, strike, protect and sustain capabilities. Finally, LandWarNet will provide one network and a single Army Battle Command system.[6]

The CIO/G6 released the memorandum, titled *Employment of Collaboration Capabilities Procedures* in 2008. Although more of a policy memorandum than a knowledge management vision, this document significantly altered the information technology acquisition process. Any collaboration requirement a command wishes to procure and join to the network must be certified and validated by NETCOM and then approved by the CIO/G6. Once certified with the Networthiness program by NETCOM, the CIO/G6 will then add it to the Approved Products List (APL). Only those products and applications on the APL can operate on the Army's network. This document effected a major change in both procurement and management. Previously commands were able to acquire their own network capabilities without input from either NETCOM or the CIO/G6.[7]

In 2007, the Army CIO/G6 published the *2008-2015 Army CIO/G6 Campaign Plan, Delivering a Joint Net-Centric Information Enterprise*. The campaign plan was an attempt to unify consolidation efforts across the Army. The goals of the campaign were to maintain a secure,

[6] Department of the Army, TRADOC Pamphlet 525-5-600, The United States Army's Concept of Operations LandWarNet 2015, (Washington, DC: Government Printing Office, 2008).

[7] Department of the Army, *Employment of Collaboration Capabilities Procedures,* (Washington, D.C.: Government Printing Office, 2008).

seamless, interdependent network through an integrated enterprise architecture. In this manner, the CIO/G6 and NETCOM could protect and defend the Army's network, ensure information management and further warfighting capabilities. This campaign stressed both the need to acknowledge information assurance as a top priority and the need to address emerging cyber security threats. Finally, the campaign recognized the existence of both an institutional garrison network and a deployed operational network. The Joint Net-Centric campaign plan would accomplish its goals while supporting both of the divergent networks.[8]

At the request of the Secretary of Defense, the Defense Science Board released the *Report of the Defense Science Board Task Force on Achieving Interoperability in a Net-Centric Environment* in 2009. The board that unit commanders procure local, non-standard software applications and purchase and employ their own servers and fiber local area networks instead of using available resources. The board also noted a need for increased bandwidth and a problem with maintaining satellite communications in more challenging environments. With regard to consolidation, the board found that users dislike systems that impose global control over their personal computers. Securing the network is also a challenge; the report found that Information Assurance training at all levels is a key to success. The board's recommendations on achieving interoperability across the Department of Defense identified five critical factors: governance, standard operating procedures, technology, training and exercise. A general lack of regulations and command and control are necessary to manage a department-wide network. Better transport capacity, through new technology, will improve access to the network. Finally, training personnel and exercising a joint network will enable the services to achieve interoperability.[9]

[8] Army CIO/G6, "2008-2015 Army CIO/G6 Campaign Plan, Delivering a Joint Net-Centric Information Enterprise," (2008), http://www.army.mil/ciog6/docs/CampaignPlan2007.pdf, (accessed September 8, 2009).

[9] Department of Defense, *Report of the Defense Science Board Task Force on Achieving Interoperability in a Net-Centric Environment.* (Washington DC: Office of the Under Secretary of Defense for Acquisition, Technology and Logistics), 2009, 1.

The CIO/G6 published *The Global Network Enterprise Construct Campaign* plan in 2009. Approved by the Chief of Staff of the Army, the campaign hopes to accomplish many of the goals outlined in previous documents. GNEC's goal is to create an enterprise that is global, standardized, protected and economical. The campaign will transform the Army's current network, which is fragmented, not standardized, unsecure and expensive. The campaign will accomplish this through the operating principles of aggregate, consolidate, standardize and modernize. The network will undergo multiple phases. Away from the current organizational structure into a federated structure consisting of large enclaves of domains. Finally, the federated network will transition to one global network.

Genesis

As computing technology transitioned from large mainframes to desk top computers throughout the 1980s, the U.S. Army Information Systems Command (ISC) was unable to adequately support local military organizations.[10] Personal computing exploded in Army organizations as the decade progressed. Organizations purchased computers and software applications to meet their own needs. As a result, a wide variety of systems, applications and networks were operating on each installation.[11] The Army established the ISC in 1984; it was given the mission consolidate communications with automation and other information management disciplines to include records management, visual information, printing and publication.[12] The ISC had detachments located at each installation; their primary mission was to manage the installation's access to the global network. Additionally, they were responsible for early information assurance and large scale procurement of computer systems and networking equipment. These ISC detachments had no customer service capabilities, further they lacked the manpower to ensure security requirements were properly followed within the organizational computing networks located on the installation.[13]

Local organizations became very frustrated with the lack of customer support the ISC detachments provided. As a result, local organizations sought their own computing solutions by purchasing more and newer systems and networking equipment.[14] This growth of more and

[10] Global Security, *NETCOM* History, www.globalsecurity.org/military/agency/army/netcom-history.htm (accessed May 7, 2010). The ISC was formerly the US Army Communication Command and was a subordinate unit to US Strategic Command.

[11] Archie Franks, The Future Role of the Director of Information Management (DOIM) Organization within the DoD Corporate Information Management Initiative. (USAWC, Carlisle Barracks, PA: 1993). 4.

[12] GlobalSecurity.org, "Network Command History," www.globalsecurity.org/military/agency/army/netcom-history.htm (accessed May 7, 2010)

[13] Donald Meynig, Donald, *Strategic Effects of the Army Enterprise Management Transformation*. (USAWC, Carlisle Barracks, PA:2002). 2.

[14] Franks, The Future Role of the Director of Information Management (DOIM) Organization within the DoD Corporate Information Management Initiative, 20.

diverse automations further exacerbated the customer support problem. Compounding the problem, the ISC detachments reported to and received their funding from ISC. The detachments did not report to the installation command. Local commanders had little ability to influence the manner in which the detachments operated. This manner of network enterprise management persisted until 1992.[15]

In 1992, Department of the Army General Order 14 established the Information Management Support Agency (IMSA) as a staff support agency under the Office of the Director of Information Systems for Command, Control and Computers. The agency was responsible for integrating interoperable and coherent information support for all Army missions.[16] That same year General Order 20 dissolved all ISC units in the continental United States.[17] The following year, the remaining ISC units were dissolved.[18] All network enterprise management responsibilities formerly overseen by the ISC detachments were now conducted by local Directorates of Information Management (DOIM) centers on each installation. These DOIMs were created from the former ISC detachments. Unlike the ISC arrangement, the commander of each DOIM reported directly to the garrison commander. Garrisons also provided funding for the DOIM.[19] The dissolution of the ISC and the transition of network enterprise management from the ISC detachments to garrison owned DOIMs was an attempt to remedy the customer support issues that had arisen over the past ten years.

The garrison DOIM approach to network management led to commanders and their organizations being well supported by a responsive automations center. While each DOIM

[15] Meynig, Strategic Effects of the Army Enterprise Management Transformation, 2-3.

[16] Department of the Army, "General Orders No. 14: Establishment of the U.S. Army Information Mission Area (IMA) Integration and Analysis Center (IIAC)" (Washington, DC: Government Printing Office, 1992).

[17] Department of the Army, "General Orders No. 20: Dissolution of U.S. Army Information Systems Command Units in the Continental United States" (Washington, DC: Government Printing Office, 1992).

[18] Department of the Army, "General Orders No. 19: Dissolution and Transfer of U.S. Army Information Systems Command Units." (Washington, DC: Government Printing Office, 1993).

[19] Meynig, Strategic Effects of the Army Enterprise Management Transformation, 4.

reported to their respective garrison commander, they also were required to report to the IMSA on technical issues. IMSA was responsible for codifying technical and information assurance standards to ensure that the Army's automations systems and networks were secure and efficient.[20] Standards were generally vague in the early and mid-nineties; enforcement of the standards rarely occurred. As a result, each installation followed its own path as local networks grew and the amount of automation equipment increased.[21] Each installation evolved along similar, yet distinct paths.

In addition to garrison DOIMs providing network enterprise management, every unit of brigade size and higher also developed their own enterprise service. This was a natural result as DOIMs do not deploy. In order to continue to maintain e-mail, web pages and other collaborative tools, a unit must have an automations systems set it can deploy with. While these networks were necessary in the field, they were not essential to maintain in garrison. DOIM was supposed to provide this enterprise service, but each unit maintained their field networks and domains while in garrison. This led to dozens of domains on each installation.[22] Army major commands and theater commander worked independently to resource their own IS requirements. This in turn led to a proliferation of non-standardized command, control, communications and computer systems and a general deregulation of Army wide information systems equipment and support networks. The deregulation led computer system incompatibility within the Army and degraded military internet operations as service users moved on beyond the original scope of simple email to the more complex environment of the worldwide web. As each unit used their own standard operating procedures in establishing and maintaining their networks, standards varied widely.[23]

[20] General Order 14.

[21] Franks, The Future Role of the Director of Information Management (DOIM) Organization within the DoD Corporate Information Management Initiative, 4.

[22] Ibid.

[23] GlobalSecurity.org, "Network Command History," www.globalsecurity.org/military/agency/army/netcom-history.htm (accessed May 7, 2010)

In an attempt to streamline enterprise services, the Department of the Army established the 9th Army Signal Command in 1996. The command was a subordinate unit of United States Forces Command. The 9th Army was given the responsibility of managing the Army's networks.[24] DOIMs still reported directly to the garrison commanders, but 9th Army established stronger standards and certifications along with a system of inspections to enforce regulations. However, in many instances organizations were unable to comply with regulations due to not knowing how to comply or being unable to comply; a problem that persist today.[25] Despite these improvements, the mass of individual networks and a lack of adherence to standards persisted, resulting in duplication of services, a lack of standardization and many security risks. Further, network interoperability between organizations and installations remained unreliable.[26]

In 2002 the Army G6 added the title of Chief Information Officer (CIO). 9th Army Signal Command was transferred from FORSCOM to the CIO/G6. In his capacity, the CIO/G6 provides architecture, governance, and operational oversight to enable joint expeditionary net-centric information dominance.[27] Between 2002 and 2008, the CIO/G6 oversaw the integration of installation DOIMs from separate geographical domains to federated bodies operating within domains organized under combatant commands and other major commands. The local DOIMs were placed under the Installation Management Authority for a short time before NETCOM assumed responsibility for managing them.

[24] Department of the Army, "General Orders No. 8: Activation of the Headquarters and Headquarters Company, 9th Army Signal Command." (Washington, DC: Government Printing Office, 1996).

[25] LandWarNet 2009, "Track 2 Information Assuarance: the Defender's Challenge, The State of Army Information Assurance," https://information assurance.us.army.mil/landwarnet/lwn2009/track%202_session_1_state%20of%20ia_ocp_final.pdf (accessed on September 8, 2009).

[26] Meynig, Strategic Effects of the Army Enterprise Management Transformation, 3.

[27] Department of the Army, "General Orders No. 5: Establishment of U.S. Army Network Enterprise Technology Command/9th Army Signal Command: Transfer and Redesignation of the Headquarters and Headquarters Company, 9th Army Signal Command; Discontinuation of the Communications Electronic Services Office and the Information Management Support Agency" (Washington, DC: Government Printing Office, 2002).

In 2006, General Order 31 tasked 9th Army Signal Command/Network Enterprise Command (NETCOM) as the lead agency for executing all globally based and expeditionary communications capabilities.[28] 9th Army Signal Command added the NETCOM title. In order to increase the efficacy and security of the Army's networks, all DOIMs fell under the Command of NETCOM. Further, each DOIM was responsible for providing all network enterprise services for the installation. Units now were forbidden to operate their own suites while in garrison. This change to the structure of the garrison networks eliminated the redundancy of unit owned and operated enterprise services and made the installation DOIM the sole entity responsible for maintaining NETCOM baseline security and operating standards.[29]

The creation of NETCOM and the new role of the DOIM, which are now known as Network Enterprise Support Centers (NESC), led to the creation of two distinct Army networks. The installation network which each unit functions within while in garrison and the operational network which units function within while deployed away from garrison. The operational network is reminiscent of the network that existed in the mid-nineties.[30] Each brigade and above operates and manages its own enterprise services. Like the installation DOIM network of the past, the operational network consist of many non-standardized networks, which are poorly regulated, redundant and insecure.[31] NETCOM has oversight of each of the networks, while consolidating services at the installation level with Network Enterprise Support Centers proved effective, given the number of distinct domains this system is not effective in the operational network.

[28] Department of the Army, "General Orders No. 31: Reinforcing the Establishment of the U.S. Army Network Enterprise Technology Command/9th Army Signal Command as a Direct Reporting Unit and Redesignating the Command as the U.S. Army Network Enterprise Technology Command/9th Signal Command (Army)" (Washington, DC: Government Printing Office, 2006).

[29] Fort Jackson Leader Staff Report, "IT Organization Changes Affiliation, Name," www.army.mil/-news/2009/10/08/28493-it-organization-changes-affiliation-name (accessed January 26, 2010.

[30] Army CIO/G6, "2008-2015 Army CIO/G6 Campaign Plan, Delivering a Joint Net-Centric Information Enterprise," (2008), http://www.army.mil/ciog6/docs/CampaignPlan2007.pdf, (accessed September 8, 2009), 10.

[31] Army CIO/G6, "Army LandWarNet: Global Network Enterprise Construct," (2009), http://www.army.mil/ciog6/docs/GNEC_2009_Trifold.pdf, (accessed on September 8, 2009), 6.

The Department of Defense's network is the Global Information Grid (GIG). The Army's portion of the GIG is known as LandWarNet. LandWarNet enables information based war fighting and support of operations regardless of operational phase or battle space circumstances. The core capabilities of LandWarNet are connect, identity, data and services. LandWarNet functions using both operational capabilities and institutional infrastructure. The goal of LandWarnet is to maintain a secure, seamless interdependent network through integrated enterprise architecture. A mission of the Army CIO/G6 is to lead integration, protect and defend networks, ensure information management and further war fighting capabilities.[32]

Despite improvements to the individual installation network, by 2007 the Army's decentralized computing environment had reached unsustainable levels from the operational, financial, technological and security perspectives.[33] While each installation support center must meet NETCOM baseline technical and security standards, not all support centers are the same. Many add additional security protocols, such as website blocking and port limitations. Further, support center servers differ between installations. In order to configure personal computers to operate on their network, support centerss image each individual computer. Imaging is an application that installs every security and administrative setting on personal computers, making every computer on the network exactly the same.[34]

Each NESC uses its own image. As a result, if a unit moves from their home station to another installation they are unable to connect to the new installation's garrison network.[35] In order to connect, each computer in the unit must have the new installation's image applied to

[32] Army CIO/G6, "2008-2015 Army CIO/G6 Campaign Plan, Delivering a Joint Net-Centric Information Enterprise."

[33] Army CIO/G6, "Army LandWarNet: Global Network Enterprise Construct," (2009), 17.

[34] The Microsoft System Center Configuration Manager 2007 client software on a master image computer is used to build computers into the NESC's enterprise. Computers built with this master image have all of thee prerequisite settings to join the enterprise. In this manner, the NESC does not have to build each computer manually. They manually build one image, then replicate it on all computers within the enterprise.

[35] 3rd Brigade Combat Team, 101st Airborne(Air Assault), OIF 07-09 After Action Report, Fort Campbell, KY: 2008.

their computer. When a computer is imaged, all of the existing data on the machine is erased. This obviously impacts a unit's computing capability. Considerable time must be spent backing up and then reinstalling all of the data lost during the imaging process. This process is repeated every time a unit moves to a new location. So, training center rotations and deployments will require a unit to erase all computer data every time it moves to a new location.

Another impact of the distinctiveness of the NESC is domain name server (DNS) application. Each post operates as a distinct DNS. DNS appears in a user's e-mail address as the xxx.FORSCOM.MIL. This address identifies the user as an authorized client on the domain to which they belong. DNS enables data traffic to find the correct recipient. DNS also enables the global address list (GAL). In order to establish a truly global address list, each DNS at every NESC must establish a trust between them. Trust between domains enables users on one domain to see and share data on another domain. Even today the Army still has between 17 and 19 active directories, active directories are enclaves of trusted domains.[36] The intent of the CIO/G6 is to get down to one active directory.[37]

These unsustainable LandWarNet problems persist within the operational network as well. The image issue applies to operational units transferring between networks as well. Each brigade and above unit maintains its own domain. The first issue is deploying to a theater. For instance, a unit deploying to Iraq will have to image any computers they connect to the network in Kuwait. Next they will have to image their networked computers with the image of the unit they are replacing. Finally, they will have to restore their own image. The process is repeated as they exit theater. While in theater, any Soldier transferring between units will have to image his computer in order to connect to another headquarters' network. Likewise, the trust issue and

[36] Nicholas Hoover, "Q & A: Army CIO Advances Consolidation Effort," *Information Week*, December 29, 2009. www.informationweek.com/story/showarticle.jhtml?artcleid=222002965 (accessed February 17, 2010).

[37] Army CIO/G6, "2008-2015 Army CIO/G6 Campaign Plan, Delivering a Joint Net-Centric Information Enterprise," (2008), 10.

multiple GALs are an especially difficult problem with the operational network in deployed areas of operations. In Iraq, each brigade and above maintains its own domain and enterprise services suite.[38] The hierarchical structure used in theater causes several difficulties.

In order for separate network domains to collaborate, a trust must be established between them. The trust enables file sharing, teleconferencing, GAL visibility and access to internal web portals.[39] In the Iraqi theater, it is very difficult to ensure trust are completed and all domains are visible and connected. This issue is easily managed at the division level by the Division Network Operations Center. Outside of the division, the network is simply too large to be effectively managed. As a result, many units are unable to communicate or collaborate over the network. Further, multiple identities exists on the network. In Iraq, older or out of date GAL entries exist for individuals along with their current entries. So, in the GAL, the same individual will appear multiple times, with only one of the entries being the correct one.[40] This is an indicator of a lack of oversight and poorly managed systems.

A new system of network management is needed to resolve these issues across the Army's Network. While the push to consolidate has progressed on the garrison network since 2001; no similar drive had been applied to the deployed networks. The issues that plagued Army Network management throughout the nineties persist today amongst the deployed forces. In addition to consolidating management on the garrison side, that management needs to applied on the deployed side. In that manner only, can the Army achieve one global network.

[38] 3rd Brigade Combat Team, 101st Airborne(Air Assault), OIF 07-09 After Action Report

[39] See Domain Name System in Appendix A: Glossary.

[40] 3rd Brigade Combat Team, 101st Airborne(Air Assault), OIF 07-09 After Action Report.

Why GNEC

Given the recognition that the Army's current use of LandWarnet is unsustainable, the CIO/G6 developed the Global Network Enterprise Construct (GNEC) to transform LandWarNet.[41] This initiative began in 2009 with the release of the CIO/G6 campaign plan, but it has its roots in the reorganization of the DOIMs, the expanded role of NETCOM and the 2008 campaign plan to deliver a joint net-centric information enterprise. The GNEC project is not being conducted only within the Army; it is a part of a whole of government approach to cyber security. The President of the United States published the Comprehensive National Cyber Security Initiative in March 2010.[42] This initiative is based upon a previous initiative studied but never published during the previous administration in 2009.

The Presidential initiative has several goals. First and foremost the government must establish a frontline defense by creating awareness of network vulnerabilities, threats and events within the federal government. The government must manage the federal enterprise network as a single network with trusted connections. The remaining preeminent goals are to establish baseline security capabilities and create a system to validate those capabilities and ensure compliance. The initiative acknowledges a lack of expertise within the government to accomplish these goals.[43] In support of this policy initiative, but released before it, the Secretary of Defense established Cyber Command as a subordinate unified command under U.S. Strategic Command.[44]

The Department of Defense recognizes that cyber space and its associated technologies offer unprecedented opportunities to the U.S. and are vital to national security. Further, the

[41] Army CIO/G6, "Army LandWarNet: Global Network Enterprise Construct" (2009) 17.

[42] Executive Office of the President of the United States, *The Comprehensive National Cybersecurity Initiative* (Washington, DC: Government Printing Office, 2010).

[43] Ibid.

[44] Department of Defense, Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations (Washington, DC: Government Printing Office, 2009).

Department's increasing dependency on cyber space, along with a growing array of cyber threats and vulnerabilities adds a new element of risk to national security. In order to secure this resource, the department requires a command that possesses the required technical capability and remains focused on the integration of cyberspace operations.[45] The primary focus of Cyber Command is to secure the Department of Defense's GIG, in that way it fits within the intent of the Presidential policy. However, it does not specifically reference the creation of a single network. The GNEC campaign, in addition to security, has the single network among its goals.[46]

The GNEC campaign developed from an earlier initiative, the CIO/G6 Campaign Plan on Delivering a Joint Net-Centric Information Enterprise. GNEC and Net-Centric share many goals. Through LandWarNet, CIO/G6 will enable information based warfighting and support operations regardless of the phase or battle space circumstances.[47] This plan was developed as the unifying strategic umbrella for the multi-dimensional effort to develop, implement and operate LandWarNet.[48] The plan delineated the roles and responsibilities of the Signal Center, NETCOM and CIO/G6. The goal of the Net-Centric campaign was to maintain a secure, seamless interdependent network through integrated enterprise architecture.[49]

Army Enterprise Architecture is: a strategic information asset base, the information necessary to perform the mission, the technologies necessary to perform the mission, the transitional process for implementing new technologies which include the current baseline architecture, the future target architecture and the sequencing plan to accomplish the target

[45] Department of Defense, Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations (2009).

[46] Army CIO/G6, "Army LandWarNet: Global Network Enterprise Construct," (2009), 4.

[47] Army CIO/G6, "2008-2015 Army CIO/G6 Campaign Plan, Delivering a Joint Net-Centric Information Enterprise" (2008), 4.

[48] Ibid, 5.

[49] Ibid, 9.

architecture.[50] In essence, Army enterprise architecture is the data, the means to transfer data and the applications to use data in support of military operations.

The Net-Centric campaign acknowledged that LandWarNet was divided into two components, operational and institutional.[51] This split is in opposition to the campaign's goal of establishing one virtual network with trusted interoperability between Combatant Commanders, Headquarters Department of the Army, and the Reserves.[52] Further, the campaign hoped to achieve everything over internet protocol (EoIP) and extend on the move data capabilities within the Brigade Combat Team (BCT) down to the company level by 2015.[53] Additionally, the campaign identified a need to address cyber security threats and maintained information assurance as a top priority.[54] Despite these worthwhile goals, the campaign did not address the fundamental structure of LandWarNet and the problems it presented. As a result, this campaign was supplanted the following year by the GNEC.[55]

Operational experience in Operation Iraqi Freedom and Operation Enduring Freedom identified the need to eliminate barriers to gain network access and allow NETCOM to establish operational control of LandWarNet. Many factors contributed for the need to pursue a new campaign for enterprise management. The intent of GNEC is to transform LandWarNet from loosely affiliated, independent networks into one with a truly global capability. The Army's current network services do not scale down to austere operational environments; as a result, users must transition from institutional to operational information services, often times loosing functionality in deployed environments. The ultimate goals of GNEC are to achieve a single universal e-mail address, universal file storage, one phone number and a standard collaboration

[50] Ibid, 6.
[51] Ibid, 10.
[52] Ibid, 10.
[53] Ibid, 10.
[54] Ibid, 7.
[55] Army CIO/G6, "Army LandWarNet: Global Network Enterprise Construct" (2009).

tool set.[56] According to the Chief of the Network Integration Division of LandWarNet, cyber security professionals disagree on the whether centralized versus decentralized is more secure, but the benefits of the centralized network from an efficiency perspective and from a protect and react perspective clearly outweigh those of a decentralized network.[57]

Cyber security concerns are a driving force behind the construct. As outlined in both the President's policy and the formation of Cyber Command, the government recognized that its networks are vulnerable. Further, government networks are not interoperable; the Department of Defense lacks an interoperable net-centric environment.[58] Increased functionality leads to increased risk. In order to attain GNEC's goal of creating a network that is truly global, it will increase the size of the population on the network. Increasing the amount of users inside the trusted network also increases the opportunities for the risk of penetration, compromise or degradation. Conventional information assurance practices practice limiting the network size and complexity. This improves security, but constrains functionality.[59] Many small enclaves of trusted domains does not guarantee security. As seen throughout the past several years with the Army's network, diverse networks are neither totally secure nor manageable.

LTG Keith Alexander, in his senate confirmation hearing, describes the nation's data networks as a strategic vulnerability. Further, he stated that improving the security of defense networks will be CyberCom's biggest challenge.[60] Only by detecting intrusions immediately, and responding to them quickly can the Army protect its data networks. The counter-argument to the small enclave approach to information assurance is visibility. In order to secure the network, the

[56] Ibid, 4-6.

[57] David Perera, "March to Consolidation."

[58] Department of Defense, *Report of the Defense Science Board Task Force on Achieving Interoperability in a Net-Centric Environment*. (Washington DC: Office of the Under Secretary of Defense for Acquisition, Technology and Logistics 2009), 1.

[59] Department of Defense, Report of the Defense Science Board Task Force on Achieving Interoperability in a Net-Centric Environment, xiv.

[60] Lolita Baldor, "Military Asserts Right to Return Cyber-Attacks," *Washington Times On-Line*, April 14, 2010. www.washingtontimes.com/news/2010/apr/14/military-asserts-right-return-cyber-attacks/ (accessed May 8, 2010).

defenders at the network operations centers must be able to see into the entire network. They attain this capability through trusted domains. Given the recognition that the signal community lacks enough trained and certified cyber security experts, returning to an enclave based security posture may not significantly lessen the risk. Any domain not administered properly is vulnerable.

The Road to GNEC

The campaign plan illustrates the current problems with LandWarNet and how these issues impact the CIO/G6's plan to achieve the campaign's goals. The current network features stove-piped: systems, processes, governance and network control. Further, the network is organizational, fragmented, not standardized, insecure and expensive. The GNEC vision is to unify LandWarNet, transforming it to deliver a global, standardized, protected and economical network enterprise. The fundamental principal behind GNEC is promoting centralized management and a decentralized execution approach to operations.[61] Ultimately the GNEC will become an enabler by effectively linking generating and operational forces from home station through training for and conducting deployed operations and back again. The core objectives of the campaign are to resolve specific LandWarNet capability gaps; improve the network defense posture; realize economies and efficiencies while improving effectiveness; and enable Army interoperability and collaboration with mission partners.[62]

In order to transform LandWarNet, the GNEC campaign will create several new organizations. These organizations will improve processes and governance. The Network Support Center provides the force a global plug and play ability to connect Army, Joint and commercial networks. The Network Support Center centralizes Network Operations of the LandWarNet Enterprise under a single entity to make it less vulnerable to attack and achieves information technology (IT) resource efficiencies.[63] The Support Center transitions the Army's Battle Command and collaboration applications and services out of the command post and individual institutions, where they are marginalized, into the enterprise where they are all available to commanders and Soldiers anywhere in the world. The Support Center provides the key connectivity interface between expeditionary operating forces and the resources of the generating

[61] Army CIO/G6, "Army LandWarNet: Global Network Enterprise Construct," (2009), 4-6.
[62] Ibid, 4-6.
[63] Ibid, 7-9.

forces. Supporting the Network Support Center construct are governance policies and activities that will create an Army-wide decision-enabling framework to ensure LandWarNet resources are managed efficiently and meet war fighter required capabilities.[64]

The Network Support Center construct is not a single, fixed organization. It is composed of distributed Fixed Regional Hub Nodes (FRHN), Area Processing Centers (APC) and Theater Network Operations and Security Centers (TNOSC).[65] The Area Processing Center is a global enterprise information processing component of the Network Support Center.[66] The processing centers are the initial step in maturing the current network that includes enhanced enterprise data management and application and services warehousing initiatives. Processing centers are located in sanctuary areas and extend common enterprise and mission services globally. Processing center are already established and operating within the continental United States and with United States Army, Europe.[67]

The remaining components of the Network Support Center are the regional hubs and the Network Operations Support Centers; The hubs provides the force a satellite to fiber interface that connects deployed operational forces to global Army, Joint and commercial network capabilities. The hub is the deployed force conduit to enterprise battle command and network service capabilities. Each of the five planned hub facilities is capable of supporting up to three Army divisions, or two divisions and five separate organizations. The hubs are located in Guam, Hawaii, the United States, Italy and Germany.[68] The Operations Centers are forward deployed, theater-based facilities that provide network operations and service desk functions to ensure

[64] Army White Paper, US.Army.Mil, "LandWarNet and the Global Information Grisd," www.army.mil/aps/08/information_papers/transform/Landwarnet_and_the_global_information_grid.html (accessed September 8, 2009).

[65] Ibid.

[66] Susan Lawrence, NETCOM/9th Signal Command (Army) 2008 AUSA Presentation. Fort Huachuca, AZ: 2008. Signal Center of Excellence, "500 Day Plan March 2008-July 2009" US Army Signal Center, (2008), www.army.mil/ciog6/docs/500DPAUG07.pdf, (accessed September 8, 2009).

[67] Ibid.

[68] Ibid.

seamless delivery of standardized enterprise services. The Operation Center is the Army's key cyber defense capability and is under the direction of the Army's Global Network Operations and Security Center. The Operations Centers are collocated with the hubs.

As mentioned earlier, GNEC is intended to unify LandWarNet. The campaign will merge the two existing networks, operational and institutional, into a single construct. This will provide many benefits to force generation and projection. As mentioned earlier, as a result of computer imaging and trust between domains, a force deploying from CONUS to a forward deployed theater will lose data and collaborative capabilities at three times: garrison to training center, training center to garrison, and garrison to deployed location. Further, each time a unit establishes an operational headquarters the G6/S6 must completely re-establish enterprise and battle command services. As a result of the institutional and operational split, this must take place throughout the generating and projection phases.[69] The hierarchical and stove-piped nature of the operational network also necessitates a complete enterprise set-up.

While in garrison, a unit headquarters pulls all enterprise services from the installation Network Enterprise Support Centers. This includes e-mail, telephone, web-portal and teleconferencing capabilities. While in a deployed environment, the headquarters uses its internal capabilities to provide these services. Each headquarters is equipped with satellite and line of site systems that provide transport capacity from the hubs. However, these internal assets are only utilized during exercises, deployments or training. Headquarters do not utilize their internal enterprise capabilities on a day-to-day basis. GNEC implementation is well underway, as operational units use the regional hubs and are protected by the operations support center.[70] The next major phase of implementation is transitioning enterprise services to the Area Processing Centers.

[69] 3rd Brigade Combat Team, 101st Airborne(Air Assault), OIF 07-09 After Action Report

[70] Barry Rosenberg, "NETCOM Focuses on Enhancing Network Service Centers," Defense Systems, October1, 2009. www.defensesystems.com/articles/2009/10/08/interview-lawrence.aspx (accessed October 12, 2009).

The need to leverage data capabilities during the train up period while a unit is in home station was demonstrated by the 82nd Airborne Division as it trained for its most recent deployment. Working with the Fort Bragg Network Enterprise Support Center, the division was able to establish its deployed domain in garrison. The G6 and Support Center developed a memorandum of agreement that enabled them to establish their enterprise services on the post. Once established, the division was able to "train as it fights." All of the capabilities and system they would use in a deployed theater were available to them in garrison for training. Further, they could establish their on-line identities before getting to theater. E-mail addresses, phone numbers and other collaboration tools on the network. This enablined the division to communicate with the elements already in theater. Establishing their domain stateside also eliminated the need to completely start fresh once in theater; they simply moved their systems and plugged them in when they arrived. All enterprise services were tested and validated prior to deploying.[71]

A unit taking actions such as these validates the need for GNEC. Commanders want the same capabilities they have while deployed while in garrison. Once GNEC is established and operational, commanders will have this capability. By hosting all services at the Area Processing Centers, the units enterprise resources are always on and always available. The units will be able to collaborate with any other unit worldwide. No longer will military units have to wait until they are deployed to establish their networks. Nor will each user have two identities, an e-mail address in garrison and a separate e-mail address while deployed. The construct recognizes the constraints put upon command and control by the current system and will alleviate those constraints by establishing an always on capability.

To support the campaign's goal of moving services from the organization and the institution to the enterprise, the campaign will move internal capacity from the organizations to

[71] Paul Sparks and Graham Fox, "A Tactical Commander's Vision of Ideal Communications," February 17, 2010. www.army.mil/-news/2010/02/17/34550-a-tactical-commanders-vision-of-ideal-communications.htm (accessed February 18, 2010).

the Area Processing Centers.[72] For a headquarters, this means they will maintain their internal transportation capacity, but will lose their internal enterprise service capacity. No longer will a headquarters need to completely re-establish its networks, they will simply connect to the GIG, either through installation Local Area Networks (LANs) or through tactical satellite communications through the regional hubs. This is plug and play capability.[73] The headquarters will maintain the exact same phone numbers, e-mail addresses and other identities wherever they are in the world, as the enterprise service provider is the fixed Area Processing Center. Further, since the domain never changes, no computers will need to be re-imaged. One image will service the organization throughout all operational phases. GNEC will have a similar impact upon institutional networks.

Institutional networks have begun the GNEC transition within the last year.[74] Garrison Network Enterprise Support Centers are broadening their domains, this is evident as installations such .camble.army.mil has switched to .forscom.army.mil. The institutional networks are expanding beyond posts to Major Army Commands (MACOM). This is the first step to moving towards one virtual network. Like the operational network, multiple domains in the Continental United States (CONUS) lead to interconnectivity issues.[75] Lack of trust between domains, imaging and multiple GALs are also an issue on the institutional network. Further, the institutional network supports each individual user on the installation, even though each user is resourced through his unit with enterprise services. For instance, user.forscom.army.mil is also user.xbct101.army.mil. This duplication of services will be eliminated when the GNEC is fully implemented.

[72] Susan Lawrence, “NETCOM/9th Signal Command (Army) 2008 AUSA Presentation,” (2009), 7.

[73] Army CIO/G6, “Army LandWarNet: Global Network Enterprise Construct,” (2009), 7.

[74] Fort Jackson Leader Staff Report, “IT Organization Changes Affiliation, Name” (2009).

[75] Army CIO/G6, “2008-2015 Army CIO/G6 Campaign Plan, Delivering a Joint Net-Centric Information Enterprise” (2008), 10.

Cyber security remains a constant concern for the Army.[76] The GNEC, in addition to streamlining enterprise service support and increasing the efficacy of LandWarNet, will improve the CIO/G6's ability to secure the network and enforce compliance with security regulations.[77] The Operations Centers guard the network, located at the regional hubs they monitor the connection point between the Theater Information Grid and the GIG. They perform the same mission in CONUS. The Operations Centers scan internal networks to ensure compliance with security standards.[78] Given the organizational nature of the current network, scanning and monitoring every computer and server in theater is an impossible task. Inspection capacity to verify compliance does not exist at the Operations Center; individual headquarters G6/S6 sections conduct inspections. In many cases, units do not know how to comply or simply cannot comply.[79] Once enterprise services have transitioned to the Area Processing Centers, it will be much easier to secure the network and ensure compliance to existing regulations.

[76] Kris Osborn, "U.S. Army Working to Ramp Up Cyber Security Efforts," *Defense News*, November 20, 2009. www.defensenews.com/story.php?i=3830717 (accessed May 11, 2010).

[77] Nicholas Hoover, "Q & A: Army CIO Advances Consolidation Effort," *Information Week*, December 29, 2009. www.informationweek.com/story/showarticle.jhtml?artcleid=222002965 (accessed February 17, 2010).

[78] 160th Signal Brigade, "SWA TNOSC Mission," (2010) www.160thsignalbrigade.swa.army.mil/TNOSC/TNOSC.html, (accessed May 11, 2010).

[79] LandWarNet 2009, "Track 2 Information Assurance; the Defender's Challenge, Components of Compliance," CIO/G6, (2009), https://informationassurance.us.army.mil/landwarnet/LWN2009/Track_2_Session_6_Panel.pdf?, (accessed on September 8, 2009).

Operation Validation

In April and May of 2009 Operation Validation (OPVAL) was the first, and only test to date, of the GNEC. The operation notionally deployed the 18th Fires Brigade from Fort Bragg to the European Command (EUCOM) area of operations. The Brigade actually deployed to the field at Fort Bragg. The intent of the operation was to validate the Network Support Center construct and measure its ability to support a brigade sized element as it prepares for combat and travels from one location to the next. The main body of the 18th Brigade's tactical operation center deployed locally, simulating a deployment to the EUCOM area of responsibility.[80] Overall, the results of the exercise were positive; however, a few key weaknesses were identified in the approach with regards to technical issues, C2 and troubleshooting issues and transport capacity.

Two Area Processing Centers supported the brigade and the EUCOM headquarters; they were located at Fort Bragg and Grafenwoehr. The FHRN at Landstuhl provided connectivity for the EUCOM command post and a CONUS based FHRN supported the brigade at Fort Bragg.[81] The brigade utilized its standard Joint Network Nodes (JNN) and Command Post Nodes (CPN) to provide data connectivity while deployed. JNNs provide up to eight megabits of data transmission capacity. During the exercise, two after action reviews noted a significant loss of incoming data traffic; further, the JNN had trouble managing the amount of traffic.[82] The amount of traffic led to applications "timing out" due to a loss of connectivity.[83] These transport shortfalls were relatively minor and similar to the amount of outages experienced by a JNN operating on the operational network.

The technical issues associated with OPVAL primarily involved transition issues and the migration of services between the processing centers. Under the construct, the servers providing

[80] David Kaplan and John Howell, "GNEC OPVAL PEO 2009 Lessons Learned" (Fort Gordon, GA: 2009), 3.

[81] Ibid, 9.

[82] Ibid, 11.

[83] John Hildebrand, "GNEC/NETCOM 2009 Lessons Learned: Austere Challenge '09/OPVAL" (Fort Gordon, GA: 2009), 4.

all enterprise services for the 18th Fires Brigade were located at the APC at Fort Bragg. The Main Tactical Operations Center, utilizing the JNNs and CPNs connected via satellite to the regional hub. The regional hub is the gateway to the LandWarNet and the GIG. The processing centers maintain a presence on LandWarNet and provide services over the network to the regional hub and the tactical satellite network. When command post forward established its tactical satellite network, it connected through the Landstuhl FHRN and, through the processing center in Grafenwohr, reached back to the service provider at Fort Bragg. During this transition establishing trusted links between the processing centers, the after action review (AAR) notes that the network did not transition seamlessly.[84] This break in communications was attributed to a complex migration process and a need for standardized training.[85]

The training issue arose as well with regards to network and hardware configuration changes. From the user in the field to the servicing processing center all network and server settings must be synchronized.[86] Wrong settings entered at any of the facilities along the transport path will result in a loss of connectivity. The AAR recommends that all configuration changes be managed and validated prior to execution.[87] The Network Operations Center (NETOPs) will manage those changes. However, the NETOPs were found to lack command and control and the CONUS and OCONUS NETOPs were not synchronized.[88] The AAR attributes these problems to a lack of standardized training and a lack of standard troubleshooting applications and processes.[89]

[84] Ibid, 7.

[85] David Kaplan and John Howell, “GNEC OPVAL PEO 2009 Lessons Learned,” 11.

[86] Ibid, 11.

[87] Ibid, 13.

[88] John Hildebrand, “GNEC/NETCOM 2009 Lessons Learned: Austere Challenge ‘09/OPVAL,” 9.

[89] Ibid, 8.

The lack of standardized tools was attributed to the delays in migrating services to the brigade as well.[90] The OPVAL did not attain seamless transitions nor did it demonstrate the ability to fight upon arrival.[91] However, these failures were the result of a loss of connectivity only for very short periods. One cause of delay in establishing service was a lack of unified DNS structure across the enterprise.[92] This results in a lack of trusts between domains and an interruption of or barrier to services. This is an acknowledged concern that GNEC is specifically designed to address. The NETOPs also lack a unified set of network management tools.[93] This contributed to a slower response time to address any loss of connectivity or services. Finally, the AAR determined that the NETOPs could not execute a "many to many" migration of units as a result of these training and standardization issues.[94]

Lastly, the removal of servers and the enterprise services they provide from unit control to APC control was a point of friction. According to one participant in the exercise, shutting down local servers with the assurance that a remote facility can do the mission just as well proved to be a "tricky proposition."[95] There was a contingent involved in the operation that lacks trust in the process. That lack of trust in the process was somewhat validated as the NETOPs supporting the units lacked a standardized trouble ticketing process.[96]

The shortfalls identified during the first OPVAL are attributed to training, a lack of standard tools and transport capacity. The successes illustrated during the exercise were the capability to maintain one identity across all phases of the operation and the successful use of the resource forest. The resource forest, or active directory forest is the outermost boundary of the

[90] David Kaplan and John Howell, "GNEC OPVAL PEO 2009 Lessons Learned," 12.

[91] John Hildebrand, "GNEC/NETCOM 2009 Lessons Learned: Austere Challenge '09/OPVAL," 4.

[92] Kaplan, David and John Howell, "GNEC OPVAL PEO 2009 Lessons Learned," 12.

[93] Ibid, 12.

[94] Ibid, 12.

[95] David Perera, "March to Consolidation," *Defense Ststems*, April 3, 2009. http://defensesystems.com/articles/2009/04/08/power-of-the-enterprise.aspx (accessed January 26, 2010).

[96] Barry Rosenberg, "NETCOM Focuses on Enhancing Network Service Centers," (2009).

directory service, all resources within the forest implicitly trust each other regardless of where they are located in the forest.[97] Utilizing the resource forest, OPVAL mitigated communications issues across domains. Further, one identity allows a user access to all of the resources in the forest with one log in and password. Leveraging the resource forest in OPVAL demonstrates GNECs capability to secure data resources and provide enterprise services to every user.

According to the exercise director, "the whole goal of the Network Support Center is that the communications infrastructure for the unit is absolutely transparent."[98] In this regard, the Network Support Center proved effective during OPVAL. The 18th Fires Brigade maintained the same computers and battle command systems they use in garrison. There was no need to image the systems. Further, by drawing services from the APC, the Brigade S6 did not have to establish a brigade domain and other mail and collaboration services. Although the elements did not demonstrate fight on arrival capabilities, the unit was able to establish their communications and enterprise services significantly faster than if they had to stand up their own servers.

[97] Microsoft, "Active Directory Forest Topologies," 2007, http://technet.microsoft.com?en-us/library/bb124765.aspx, (accessed May 1, 2010)

[98] David Perera, "March to Consolidation," (2009).

Lessons Learned

The need for effective governance of the Army's networks is addressed in both the Net-Centric Campaign Plan and the Subsequent Global Network Enterprise Construct plan. The impacts of governance cover a wide scope of activities at all levels of the Army. These activities range from user and administrative training to standardized applications. These deficiencies were evident in Operation Validation. Governance encompasses training, regulations, equipment and enforcement of the applicable standards. Training with new technology is a challenge for any organization; in regards to information assurance and user training, the Army is implementing a sound program.

All users on the military network are required to complete on-line training and testing annually. This program's purpose is to secure the Army's network from cyber security threats.[99] Where the Army has fallen behind in training is with the administrators and security experts responsible for securing and maintaining the network. As is evident in the campaign plans and demonstrated during OPVAL, communications personnel from the brigade combat team to the processing centers lack the professional training to execute the seamless transitions throughout all phases that GNEC promises. Without a standardized training program implemented and validated at the Signal Center, a lack of sufficient training will persist within the profession. The Army Signal Center has taken steps to address this concern.[100] Centers of excellence, industry professional certifications, and continuing education through on-line training are valuable tools to train the force; however, a mechanism must be in place to certify those communicators.

Regulations governing the network are critical to success. *Army Regulation 25-1, Army Knowledge Management and Information Technology* and *Army Regulation 25-2, Information Assurance* proscribes the roles and responsibilities of individuals and organizations with regard to

[99] Department of the Army, *AR 25-1, Army Knowledge Management and Infromation Technologies* (Washington, DC: Government Printing Office, 2008). 30.

[100] Signal Center of Excellence, "500 Day Plan March 2008-July 2009," (US Army Signal Center, 2008), www.army.mil/ciog6/docs/500dpaug07.pdf, (accessed September 8, 2009).

network activities. Further, Approval to Operate memorandums between organizations and NETCOM ensure all organization meet minimum security standards.[101] These regulations serve the community effectively, but what the community lacks is a standardized regulation governing establishing and joining the network. As shown in OPVAL, the two separate processing centers had significant command and control issues. Further, the processing centers used different tools and applications to conduct troubleshooting and network monitoring functions. As GNEC matures, suitable regulations governing the organization will emerge, but until they do the problems of OPVAL will persist.

Finally, enforcement of established regulations is necessary to achieve the goals of GNEC. Currently, higher headquarters G6/S6 sections are responsible for inspecting units to ensure compliance with the regulations. In most cases, these personnel lack the training and background to adequately assess their subordinate organizations. As enterprise services transition from units to the processing centers, this will become less of an issue. However, ensuring compliance at the user level is equally important as securing the domains. NETCOM will need a means of enforcing security standards across the entire network from the user level upward. Until this can be implemented, security breaches will continue.

The Signal Center, Defense Science Board and OPVAL demonstrated the inadequate transport capacity of current satellite communications assets. The board found a need for increased bandwidth.[102] Similarly, the Signal Center acknowledges that the current systems are inadequate.[103] During OPVAL, bandwidth restrictions resulted in a loss of data and connectivity. While deployed, most brigade combat teams purchase commercial off the shelf line of site transmission systems in order to support their data needs and serve as a back-up to the

[101] Department of the Army, *AR 25-2, Information Assurance*. (Washington, DC: Government Printing Office, 2009). 50.

[102] Department of Defense, *Report of the Defense Science Board Task Force on Achieving Interoperability in a Net-Centric Environment* (Washington DC: Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, 2009) xiii.

[103] Signal Center of Excellence, "500 Day Plan March 2008-July 2009"

organization's satellite communications assemblages.[104] GNEC hopes to realize on the move data capability at the company level by 2015; using current systems, this is an unattainable goal. Our current set of JNN and CPN support static data to the battalion level. In those instances where companies are supported, it is through commercial off the shelf equipment. Lack of bandwidth will continue to plague the force for the foreseeable future.

Another impact of OPVAL is the loss of enterprise service in the operational force. The 18th Fires Brigade relied upon the same suite of tools available to them in garrison. While the time to establish the network was greatly diminished, the brigade was forced to use trouble tickets to resolve any issue with enterprise services. Under the current operational network, the unit G6/S6 owns maintains and operates the servers. Should a new user need access or a user lost his password, the unit communications section can quickly resolve the issue. Under the construct, the user would go to the G6 and complete an online trouble ticket. This ticket then goes to the processing center or operations center where an administrator resolves it. This loss of power was difficult for a segment of the units that participated in OPVAL.[105]

Transport capacity, training and a lack of standard operating procedure undermined the construct's ability to support the brigade at the desired levels. This prevented the brigade from achieving a true fight on arrival capability and delivered less than true plug and play capability. However, the construct did effectively transition enterprise services from garrison to a deployed environment. The construct also allowed the brigade to train as it fights, by delivering the same network capabilities the brigade uses in garrison. Finally, OPVAL revealed the command's reticence to surrender a capability. An element of the supported brigade did not trust their resource needs could be met by an outside organization. This lack of trust was somewhat

[104] A brigade combat team only has an MTOE of communications assemblages to support each battalion headquarters and a main and forward brigade command post. In order to link additional command posts, brigades use commercial off the shelf microwave line of sight systems to provide connectivity to below battalion level.

[105] David Perera, "March to Consolidation."

confirmed when the construct failed to deliver in some areas. In order to implement the construct, the signal community must have the trust of the supported unit.

Future Friction

The current CIO/G6, LTG Jeffrey Sorensen mentioned the need for communication professionals to manage their customers expectations.[106] Expectation management is a tacit recognition of the limitations of both the Army's current and future network enterprise. Given the experience of OPVAL, the unit G6 must ensure the commander knows the limitations of transport capacity, migration time and trouble shooting procedures. Each of these were problematic during the exercise and have the potential to remain a problem throughout the implementation of GNEC. Managing the commander's expectations is particularly important given the Global Network Enterprise Construct, this is because commanders will no longer own their own enterprise service hardware; they must rely upon the TNOSC and APC to provide enterprise services. In order to assuage the trepidation commanders feel at the loss of their equipment, NETCOM must standardize and publish procedures.

The DoD Science Board included a lack of standard operating procedures (SOP) as a concern with the current joint network.[107] A lack of standard procedures makes expectation management difficult. Trouble shooting and trouble ticketing procedures have to remain consistent in all geographical areas. That is not the case now, as demonstrated during OPVAL. A G6 will be unable to ensure his commander is satisfied with the support he receives from NETCOM if every network outage is resolved in a different manner every time. Further, if trouble ticket applications differ between geographic areas the G6 will have a difficult time in managing his users. In order to manage expectations, the G6 will need an SOP and a consistent

[106] Nicholas Hoover, "Q & A: Army CIO Advances Consolidation Effort," *Information Week*, December 29, 2009. www.informationweek.com/story/showarticle.jhtml?artclid=222002965. (accessed February 26, 2010.

[107] Department of Defense, Report of the Defense Science Board Task Force on Achieving Interoperability in a Net-Centric Environment, xiii.

trouble resolving system. Further, this will work towards NETCOMs goal of making the communications infrastructure invisible to the user.[108]

The G6 must also manage expectations with regard to transport capacity. As was demonstrated during OPVAL, our current satellite communications systems cannot maintain 100% reliability. Even when a communication link is fully operational, there is still a possibility data will be lost due to lag time.[109] The G6 must ensure his commander understands the limitations of our operational communications architecture. JNNs effectively manage all enterprise services, CPNs do not. The G6 must ensure the commander is aware that applications such video teleconferencing and large file transfers are often not possible with subordinate units supported only by a CPN. Commanders often time overcome these limitations by purchasing commercial of the shelf systems and integrating them into the network. This approach will no longer be an option as the Army transitions to the construct as a result of increased security measures.

As security restrictions increase and fall under the management of the TNOSC and NETCOM, many capabilities the commander has today may be lost. Expectation management is especially critical in this area. Webpage blocking is a common filter applied to military units on all of the network.[110] During times of increased threat or limited connectivity, the NOSC can increase the filter to exclude pages that were allowed previously. Further, many pages the intelligence sections utilize for open source, such as Jihadi pages, are blocked by the filter. NETCOM must publish and distribute its procedures in reference to changing security levels in order for the G6 to keep his commander informed. Further, NETCOM must have an exemption

[108] Peter Buxbaum, "Army CIO Talks Transformation," *Federal Computer Weekly*, January 31, 2008. http://fcw.com/articles/2008/01/31/army-cio-talks-transformation.aspx (accessed October 12, 2009).

[109] A communication link may be fully connected and passing data packets, but if there is latency along the path, services such as video or large file transfers will fail. Latency is the time delay inherent in satellite transmission as the user reaches back over the link to the hub and in to the GIG.

[110] Each TNOSC in the Army uses a filter to ensure only appropriate web sights can be accessed by users. The filter limits access to sites which may be security threats and other sites which may be against Army Regulations.

program to allow the gathering of open source. The current exemption program varies depending on geographical location.[111]

Security concerns also apply to applications and hardware a unit may use to support its mission. These applications are easily supported by the G6 while deployed; the G6 owns his network. However, as GNEC develops the G6 will lose his network and become dependent upon the Network Support Center. Applications used for logistic and medical support must now be approved, hosted and managed at the Area Processing Center.[112] NETCOM must ensure a validation process is published in order for the G6 to meet his commander's data needs. Currently, the G6 is the validating authority for non-standard software applications. In the same manner, the G6 will no longer validate what hardware can be connected to the network. Any new hardware, such as cameras, smart phones and storage drives must be approved by the NOSC. To serve the commander, the G6 must know what hardware he can purchase to fulfill the capability the unit needs. A published SOP is critical for this task.

Commanders have an expectation of a high quality data network. LTG Austin recently commented "I deploy to Iraq and I have superior communications support. I redeploy to Fort Bragg and I return to the stone ages." He goes on to say "we must have the same network we fight with back at home station."[113] A future point of friction for GNEC is that the Army is doing the exact opposite of what LTG Austin is asking for. While it is going to be one network, it will not be the same network. We are bringing the network from home station to replace the network we fight with. Replacing the network we fight with is a necessary action, as the current operational versus institutional architecture is unsustainable, but there can be concern that we are creating DOIMs down range – bringing the stone age forward when what the Army fights with

[111] Department of the Army, AR 25-2, Information Assurance.
[112] David Perera, "March to Consolidation."
[113] John Hildebrand, "GNEC/NETCOM 2009 Lessons Learned: Austere Challenge 09/OPVAL."

now is considered superior. In order to overcome this natural resistance to change, the signal community must ensure the users trust the organization.

LTG Sorensen has spoken in interviews with the regard to the need of the signalers to establish trust with their clients.[114] The community must ensure that commanders and users trust that others will take care of them as well as they have taken care of themselves. To accomplish this, the signal community must provide responsive customer service, reliable enterprise support and deliver the services the user expects. It begins with published standards that delineates responsibilities between organizations and uses a standard set of applications that make the network's infrastructure invisible to the user.

Responsive customer service is essential if the signal community wishes to establish trust with their clients. The help desk will be operated from the NOSC under the construct. This help desk must be appropriately manned in order to satisfy the client. Further, the NOSC should publish an expected turn around time for frequent problems. Additionally, the G6 and his section should be given permission to perform common trouble shooting procedures. Permissions to install hardware or add and manages network user accounts will enable both the NOSC and the G6 to resolve issues quickly. The G6 can manage the local issues thus reducing the workload on the NOSC.

Reliable enterprise support will also foster trust. Collaboration tools, e-mail and web portal support are critical to the day-to-day functions of all military organizations. In the Army's current structure, a commander may add capacity and applications with only the G6's approval. Purchasing an additional Exchange or Adobe connect server in order to increase the amount of Soldiers on the network or adding a teleconferencing capacity is a common example. The GNEC will remove this resource from commanders. The clients will trust the signal community only if

[114] Nicholas Hoover, "Q & A: Army CIO Advances Consolidation Effort."

we can meet his needs. As LTG Austin comments show, commanders have a high expectation for support; GNEC must meet those expectations.

Commanders will not trust the construct if it fails to deliver at least the same capabilities they have grown accustomed to. Reliability and flexibility are two of the hallmarks of the operational network. GNEC will remove the commander's ability to leverage his own assets to solve capability gaps and it will eliminate his ability to reach out and grab his G6. The dissatisfaction with this type of support is demonstrated by LTG Austin's "stone age" comment. In order to establish trust and maintain reliability, flexibility and responsiveness, the TNOSC must be readily available and a partner with the G6s they support. If the construct does not meet the commander's needs and fulfill his expectations, he will lose faith in both his G6 and the construct.

Since the current operational system is satisfying commander's needs, the signal community must convey to the clients why they need a new system. Security, reliability, and fiscal efficiencies are the primary factors behind the transition to GNEC. The community must ensure our leaders are broadcasting the message to the Army's senior leadership. The campaign plan mentions the need for the community to sell the need for the transition. The unit level G6 and S6 must also be a part of this campaign. Although a new initiative, the GNEC is relatively unknown outside of the participants in the transition within NETCOM. At a recent college visit to Fort Leavenworth, the Chief of Signal did not even address the plan. Knowing what is ahead is critical to the success of G6s; they must adapt to the changing system and ensure their commander's expectations are met.

Appendix A: Glossary

Area Processing Center: The centers provide common enterprise information technology (IT) services and applications hosting for battle command, intelligence, and business systems.

Command Post Node: The CPN provides enhanced voice and data capabilities support to battalion headquarters. The CPN is a smaller, less capable version of the JNN. Utilizing a Ku Band satellite, the CPN provides data services by linking in with the JNN.

Domain Name System: The Domain Name System (DNS) is a hierarchical naming system for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participants. Most importantly, it translates domain names meaningful to humans into the numerical (binary) identifiers associated with networking equipment for the purpose of locating and addressing these devices worldwide. An often-used analogy to explain the Domain Name System is that it serves as the "phone book" for the Internet by translating human-friendly computer hostnames into IP addresses. For example, *www.example.com* translates to *192.0.32.10*. The Domain Name System makes it possible to assign domain names to groups of Internet users in a meaningful way, independent of each user's physical location. Because of this, World Wide Web (WWW) hyperlinks and Internet contact information can remain consistent and constant even if the current Internet routing arrangements change or the participant uses a mobile device. The Domain Name System distributes the responsibility of assigning domain names and mapping those names to IP addresses by designating authoritative name servers for each domain. Authoritative name servers are assigned to be responsible for their particular domains, and in turn can assign other authoritative name servers for their sub-domains. This mechanism has made the DNS distributed and fault tolerant and has helped avoid the need for a single central register to be continually consulted and updated. In general, the Domain Name System also stores other types of information, such as the list of mail servers that accept email for a given Internet domain. By providing a worldwide, distributed keyword-based redirection service, the Domain Name System is an essential component of the functionality of the Internet. The Domain Name System also defines the technical underpinnings of the functionality of this database service. For this purpose it defines the DNS protocol, a detailed specification of the data structures and communication exchanges used in DNS, as part of the Internet Protocol Suite (TCP/IP).

Everything over IP (EoIP): “Everything over IP” can be understood in two different ways, and both ways are important. First, in terms of transport protocols, IP is the clear winner over existing transport protocols. The acceptance of a uniform network layer, together with the corresponding transport protocols, fuelled the creation of a vast number of services to be run on top of it. With this in mind, the WWW is the natural extension of IP, and acted as a “booster” for the public

Internet. The growth of IP-based Virtual Private Networks (VPNs) will contribute to the phasing out of the costly circuit-based private networks: IP-VPNs are ubiquitous because they extend beyond Frame Relay or Asynchronous Transfer Mode networks, and the deployment costs of IP-VPNs are significantly lower than for similar technologies. The second and more direct interpretation of the title shows how all known transport technologies are nowadays used to carry IP packets, from switched circuits to shared wireless LANs, from optical wavelenghts to cable TV networks. But paradoxically, most of these technologies were not developed from scratch to specifically support IP packets. Instead, they were either developed to respond to consequences of the success of IP, namely the growth of data traffic, or retro-fitted to accommodate the ubiquitousness of IP. A network designed for IP has yet to come. Clearly, given the wide range of services running on top of IP, enhancements are required, such as header compression for better voice support, Quality of Service for predictable delays and bandwidth, security to allow business transactions to take place safely, and billing mechanisms, to name just a few. This will eventually make IP a more complex protocol, and may lead to dedicated alternatives being preferred in specific cases.

Fixed Regional Hub Nodes: Hub nodes provide a direct link to the Global Information Grid.

Global Address List: The Global Address List, also known as Microsoft Exchange Global Address Book is a directory service within the Microsoft Exchange email system. The GAL contains information for all email users, distribution groups, and Exchange resources. Digital IDs certificates generated by Microsoft Exchange Server Advanced Security IIS or by Microsoft Exchange Key Management Server (KMS) are automatically published in the Global Address Book. Users of Microsoft Outlook can publish to GAL their externally generated PKI certificates that are used for secure e-mail.

Global Information Grid: The Global Information Grid (GIG) is the globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to Soldiers, policy-makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve information superiority. The GIG supports all Department of Defense (DoD), national security, and related intelligence community functions in war and in peace.

Global Network Enterprise Construct: Inefficiencies and capability gaps in LandWarNet require the Army to transform LandWarNet using the GNEC to improve efficiencies, raise effectiveness, enable fighting capabilities, dramatically improve network defense, and make the Army interoperable with other military departments throughout the Department of Defense (DoD). The GNEC integrates several ongoing network enterprise programs and new initiatives into a single strategy to ensure global connectivity under one network manager. Using GNEC to organize the Army's information will make it globally accessible and useful to Soldiers world-wide. The GNEC is an Army-wide strategy to unify LandWarNet as an Army enterprise activity. The GNEC is an integrating construct to bring LandWarNet and battle command programs and initiatives into theater-based alignment with this enterprise objective. The central component of the GNEC strategy is Network Service Centers (NSC). The Army will establish an NSC within each theater to achieve four strategic objectives: enable warfighting capabilities through the network, dramatically improve LandWarNet defense posture, realize efficiencies while improving effectiveness and ensure Army interoperability across the DoD.

Joint Network Node: The JNN is commercial equipment packaged in tactical shelters that may be likened to an internet department on wheels. This differs from legacy equipment in the tactical communications architecture, virtually all of which was uniquely built for the military. The commercial components of JNN are used for both strategic and tactical communications. The commercial names on the components inside the S-250 shelter of the JNN terminal are like any other network facility in the commercial world or on any fixed-station military installation. These Cisco™ routers and Promina™ switches are non-developmental items. JNN consists of vehicles equipped with satellite communications as well as voice-over-IP and dynamic IP technologies and systems that connect to military networks. One 2.4M dish Ku band satellite transportable terminal (STT) is fielded with the JNN to provide direct reach back capabilities to higher command and or strategic enclaves. The JNN can provide up to 3 Mbps FDMA satellite communications and is capable of shared bursts up to 4 Mbps to the Command Post Nodes. The JNN supports user interfaces into NIPRNET and SIPRNET data networks.

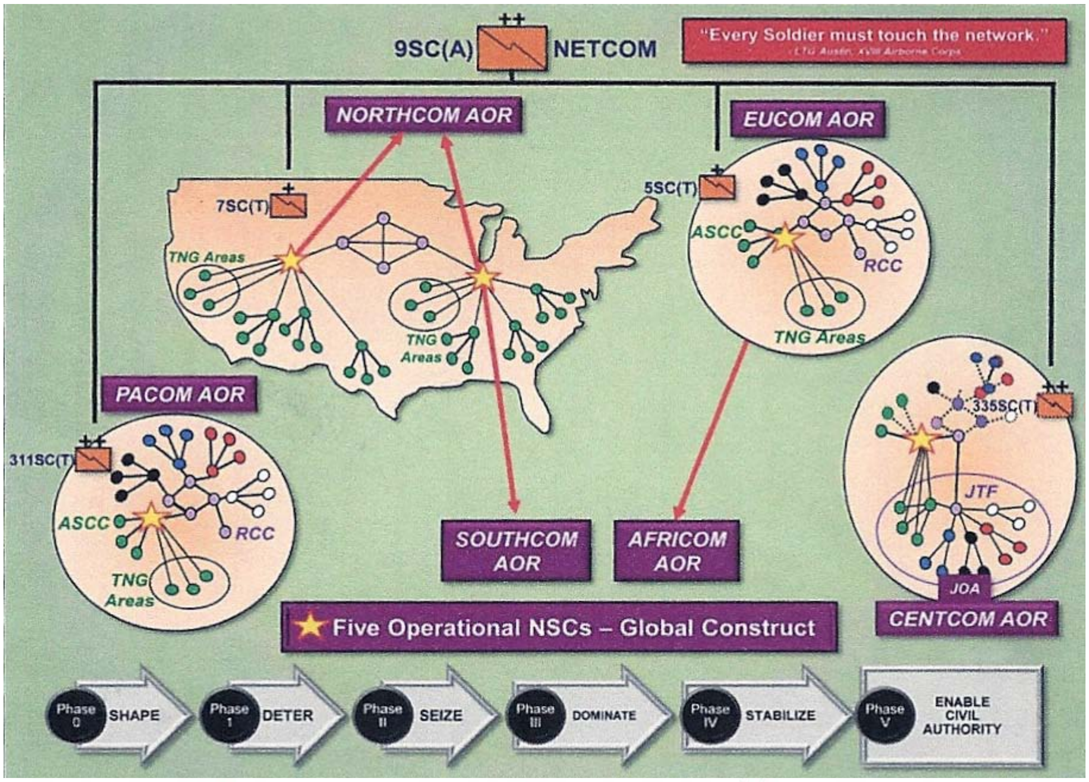
LandWarNet: LandWarNet is the Army's portion of the GIG. A combination of infrastructure and services, it moves information through a seamless network and enables the management and use of warfighting and business information. For strategic oversight, the development of LandWarNet has been divided into two strategic initiatives: (1) developing the LandWarNet institutional infrastructure, which encompasses the network, applications, and information technology (IT) processes that support Army institutions (the generating force); and (2) developing LandWarNet operational capabilities, which includes network capabilities, applications, and processes that directly support the operating force.

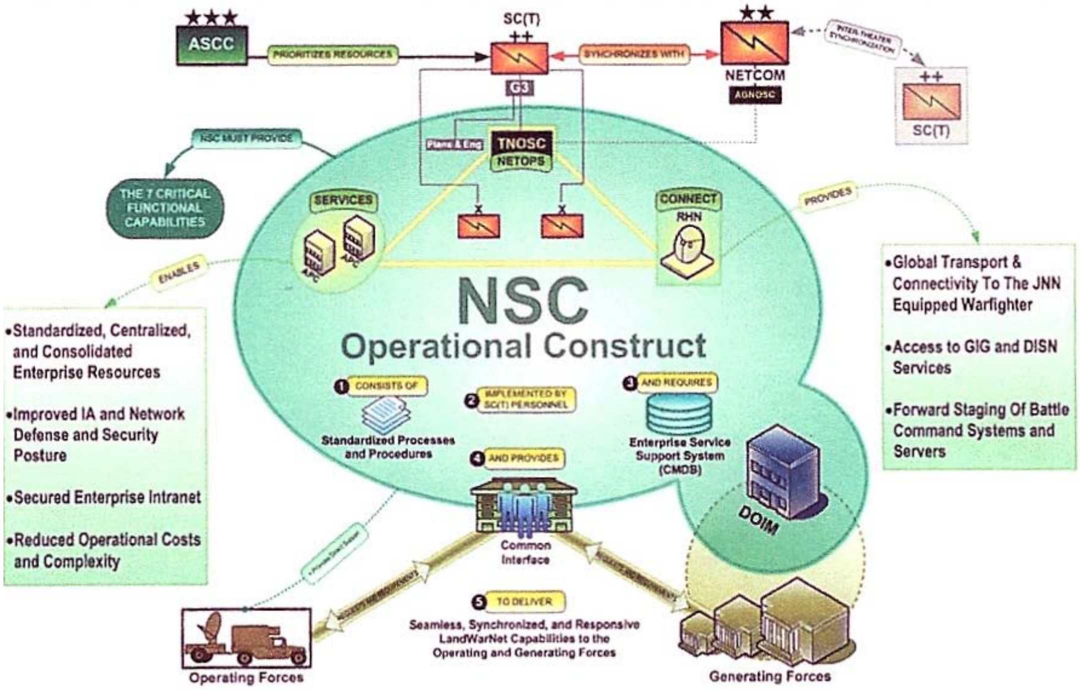
Network Enterprise Support Center: Formerly known as the Directorate of Information Management (DOIM); these facilities support and are located on each Army installation, they provide enterprise services and support the APCs

Network Support Center: the NSC is an integration of geographically separated network capabilities that provide economies and efficiencies of enterprise services for the Army. The NSC is made up of the APCs, the FHRNs and the NOSC.

Network Operations Support Centers: the single enterprise network manager who provides network command and control, network operations and services in support of the Army.

Appendix B: The Global Network Enterprise Construct




ASCC
PRIORITIZES RESOURCES
SC(T)
SYNCHRONIZES WITH
NETCOM
AGNOSC
INTER-THEATER SYNCHRONIZATION
SC(T)
G3
NSC MUST PROVIDE
THE 7 CRITICAL FUNCTIONAL CAPABILITIES
Plans & Eng
TNOSC
NETOPS
SERVICES
APC
APC
CONNECT
RHN
PROVIDES
ENABLES
NSC
Operational Construct
1 CONSISTS OF
Standardized Processes and Procedures
2 IMPLEMENTED BY SC(T) PERSONNEL
3 AND REQUIRES
Enterprise Service Support System (CMDB)
4 AND PROVIDES
Common Interface
DOIM
5 TO DELIVER
Seamless, Synchronized, and Responsive LandWarNet Capabilities to the Operating and Generating Forces
Operating Forces
Generating Forces

- Standardized, Centralized, and Consolidated Enterprise Resources
- Improved IA and Network Defense and Security Posture
- Secured Enterprise Intranet
- Reduced Operational Costs and Complexity

- Global Transport & Connectivity To The JNN Equipped Warfighter
- Access to GIG and DISN Services
- Forward Staging Of Battle Command Systems and Servers

BIBLIOGRAPHY

3rd Brigade Combat Team. 101st Airborne(Air Assault), OIF 07-09 *After Action Report*, Fort Campbell, KY: 2008.

Army CIO/G6. “2008-2015 Army CIO/G6 Campaign Plan, Delivering a Joint Net-Centric Information Enterprise,” www.army.mil, 2008, http://www.army.mil/ciog6/docs/CampaignPlan2007.pdf, (accessed September 8, 2009).

Army CIO/G6. “Army LandWarNet: Global Network Enterprise Construct,”www.army.mil, 2009, http://www.army.mil/ciog6/docs/GNEC_2009_Trifold.pdf, (accessed on September 8, 2009).

Army CIO/G6. “Global Network Enterprise Construct: The Army’s Strategic Vision for the Transformation of LandWarNet,” www.army.mil, 2009, http://www.army.mil/ciog6/docs/GNEC_2009_Brochure.pdf, (accessed on September 8, 2009).

Buxbaum, Peter. “Army CIO Talks Transformation,” *Federal Computer Week*, January 31, 2008. http://fcw.com/articles/2008/01/31/army-cio-talks-transformation.aspx (accessed October 12, 2009).

Baldor, Lolita. “Military Asserts Right to Return Cyber-Attacks,” *Washington Times On-Line*, April 14, 2010. www.washingtontimes.com/news/2010/apr/14/military-asserts-right-return-cyber-attacks/ (accessed May 8, 2010).

Department of the Army. *AR 25-1*, *Army Knowledge Management and Information Technology*. Washington, D.C.: Government Printing Office, 2008.

Department of the Army. *AR 25-2, Information Assurance*. Washington, DC: Government Printing Office, 2009. 50.

Department of the Army. *The Army Knowledge Management Implementation Plan*, Washington, D.C.: 2003.

Department of the Army. “Army Knowledge Management Guidance Memo #1,” Washington D.C.: Government Printing Office, 2001.

Department of the Army. “Army Knowledge Management Guidance Memo #2,” Washington D.C.: Government Printing Office, 2001.

Department of the Army. “Army Posture Statement, www.army.mil, 2006,” 2006, http://www.army.mil/aps/06/01_index.html, (accessed September 8, 2009).

Department of the Army. “Army Posture Statement, 2007,” www.army.mil, 2007, http://www.army.mil/aps/07/, (accessed September 8, 2009).

Department of the Army. “Army Posture Statement, 2008,” www.army.mil, 2008, http://www.army.mil/aps/08/, (accessed September 8, 2009).

Department of the Army. “Army Posture Statement, 2009,” www.army.mil, 2009, http://www.army.mil/aps/09/, (accessed September 8, 2009).

Department of the Army. “Employment of Collaboration Capabilities Procedures,” Washington, D.C.: Government Printing Office, 2008.

Department of the Army. *Enterprise Network Operations (NetOps) Integrated Architecture Implementation*. Washington, DC: Government Printing Office, 2008.

Department of the Army. *General Orders No. 14: Establishment of the U.S. Army Information Mission Area (IMA) Integration and Analysis Center (IIAC)*. Washington, DC: Government Printing Office, 1992.

Department of the Army. *General Orders No. 19: Dissolution and Transfer of U.S. Army Information Systems Command Units*. Washington, DC: Government Printing Office, 1993.

Department of the Army. *General Orders No. 20: Dissolution of U.S. Army Information Systems Command Units in the Continental United States*. Washington, DC: Government Printing Office, 1992.

Department of the Army. *General Orders No. 31: Reinforcing the Establishment of the U.S. Army Network Enterprise Technology Command/9th Army Signal Command as a Direct Reporting Unit and Redesignating the Command as the U.S. Army Network Enterprise Technology Command/9th Signal Command (Army)*. Washington, DC: Government Printing Office, 2006.

Department of the Army. *General Orders No. 5: Establishment of U.S. Army Network Enterprise Technology Command/9th Army Signal Command: Transfer and Redesignation of the Headquarters and Headquarters Company, 9th Army Signal Command; Discontinuation of the Communications Electronic Services Office and the Information Management Support Agency*. Washington, DC: Government Printing Office, 2002.

Department of the Army. *General Orders No. 8: Activation of the Headquarters and Headquarters Company, 9th Army Signal Command*. Washington, DC: Government Printing Office, 1996.

Department of the Army. *General Orders No. 7: Unit Redesignation/Reassignment of the U.S. Army Information Systems Command*. Washington, DC: Government Printing Office, 1996.

Department of the Army. *The Single DOIM Action Plan for Command, Control, Communications, Computers and Information Management (C4IM) Common User Services*. Washington, D.C.: Government Printing Office, 2006.

Department of the Army. *TRADOC Pamphlet 525-5-600, The United States Army's Concept of Operations LandWarNet 2015*. Washington, DC: Government Printing Office, 2008.

Department of Defense. *Department of Defense Directive (DoDD) 5144.1, Assistant Secretary of Defense for Networks and Information Integration DoD Chief Information Officer (ASD(NII)/DoD CIO)*. Washington, DC: Government Printing Office, 2005.

Department of Defense. *Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations*. Washington, DC: Government Printing Office, 2009.

Department of Defense. *Report of the Defense Science Board Task Force on Achieving Interoperability in a Net-Centric Environment*. Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, 2009.

Department of the Navy Chief Information Officer. "Interview with Mag. Gen. Susan Lawrence, Commanding General U.S. Army Network Enterprise Technology Command," www.chips.navy.mil, 2009, www.chips.navy.mil/archives/09_oct/web_pages/mgen_lawrence.html, (accessed May 1, 2010)

Executive Office of the President of the United States. *The Comprehensive National Cybersecurity Initiative*. Washington, DC: Government Printing Office, 2010.

Franks, Archie, *The Future Role of the Director of Information Management (DOIM) Organization within the DoD Corporate Information Management Initiative*. Carlisle Barracks, PA: United States Army War College, 1993.

Fort Jackson Leader Staff Report. "IT Organization Changes Affiliation, Name," *Fort Jackson Leader*, 2009, www.army.mil/-news/2009/10/08/28493-it-organization-changes-affiliation-name (accessed January 26, 2010).

GlobalSecurity.org. "Network Command History," *Global Security*, 2009, www.globalsecurity.org/military/agency/army/netcom-history.htm (accessed May 7, 2010).

Hildebrand, John. *GNEC/NETCOM 2009 Lessons Learned: Austere Challenge '09/OPVAL*. Fort Gordon, GA: 2009.

Hoover, Nicholas. "Q & A: Army CIO Advances Consolidation Effort," *Information Week*, December 29, 2009. www.informationweek.com/story/showarticle.jhtml?artcleid=222002965 (accessed February 17, 2010).

Kaplan, David and John Howell. *GNEC OPVAL PEO 2009 Lessons Learned*. Fort Gordon, GA: 2009.

LandWarNet 2009. "Track 2 Information Assurance; the Defender's Challenge, Components of Compliance," CIO/G6, 2009, https://informationassurance.us.army.mil/landwarnet/LWN2009/Track_2_Session_6_Panel.pdf?, (accessed on September 8, 2009).

LandWarNet 2009. "Track 2 Information Assurance; the Defender's Challenge, The State of Army Information Assurance," CIO/G6, 2009, https://informationassurance.us.army.mil/landwarnet/LWN2009/Track%202_Session_1__State%20of%20IA_OCP_Final.pdf, (accessed on September 8, 2009).

Lawrence, Susan. *NETCOM/9th Signal Command (Army) 2008 AUSA Presentation*. Fort Huachuca, AZ: 2008.

Signal Center of Excellence. "500 Day Plan March 2008-July 2009," US Army Signal Center, 2008, www.army.mil/ciog6/docs/500DPAUG07.pdf, (accessed September 8, 2009).

McConnel, Mike. "Mike McConnel on How to Win the Cyber-War We are Losing," *The Washington Post*, February 28, 2010. www.washingtonpost.com/wp-dyn/content/article/2010/02/25/ar2010022502493_pf.html (accessed February 28, 2010).

Meynig, Donald. *Strategic Effects of the Army Enterprise Management Transformation*. USAWC, Carlisle Barracks, PA:2002.

Microsoft. "Active Directory Forest Topologies," www.technet.microsoft.com, 2007, http://technet.microsoft.com?en-us/library/bb124765.aspx, (accessed May 1, 2010)

Osborn, Kris,."U.S. Army Working to Ramp Up Cyber Security Efforts," *Defense News*, November 20, 2009. www.defensenews.com/story.php?i=3830717 (accessed May 11, 2010).

Perera, David. "March to Consolidation," *Defense Systems*, April 3, 2009. http://defensesystems.com/articles/2009/04/08/power-of-the-enterprise.aspx (accessed January 26, 2010).

Rosenberg, Barry, “Army Enterprise Chief Outlines Network Modernization Efforts,” *Defense Systems*, July 2, 2009. www.defensesystems.com/articles/2009/07/08/interview-with-army-peo-eis-gary-winkler.aspx (accessed October 12, 2009).

Rosenberg, Barry. “NETCOM Focuses on Enhancing Network Service Centers,” *Defense Systems*, October1, 2009. www.defensesystems.com/articles/2009/10/08/interview-lawrence.aspx (accessed October 12, 2009).

Sparks, Paul and Graham Fox. “A Tactical Commander’s Vision of Ideal Communications,” www.army.mil, February 17, 2010. www.army.mil/-news/2010/02/17/34550-a-tactical-commanders-vision-of-ideal-communications.htm (accessed February 18, 2010).

U.S. Government Accountability Office. “B-292182, Remtech Services, Inc., July 17, 2003,” *GAO*, 2003, www.gao.gov/decisions/bidpro/292182.htm, (accessed January 12, 2010).